[520.1007]

METHOD FOR ESTABLISHING A COMMON KEY FOR A GROUP OF AT LEAST THREE SUBSCRIBERS

(2) What is claimed is:

1. A method for establishing a common key for a group of at least three subscribers, using a publicly known mathematical group G and a publicly known element of the group g ∈ G of large order,

wherein

a) each subscriber (Ti) generates a message (Ni = g^{zi} mod p) from the publicly known element (g) of the group (G) and a random number (zi) selected or generated by him/her and sends it to all other subscribers (Tj),

b) each subscriber (Ti) generates a transmission key (k^{ij}) from the messages (Nj) received from the other subscribers (Tj, j ≠ i) and his/her random number (zi) according to the function k^{ij}: = $Nj^{zi} = (g^{zj})^{zi}$, the key being also known to subscriber (Tj) due to the equation $k^{ij} = k^{ji}$,

c) each subscriber (Ti) sends his/her random number (zi) to all other subscribers (Tj) in encrypted form by generating the message (Mij) according to Mij := E(k^{ij}, zi), with E(k^{ij}, zi) being a symmetrical encryption algorithm in which the data record (zi) is encrypted with the common transmission key (k^{ij}), and

d) the common key (k) to be established is determined by each subscriber (Ti) from his/her own random number (zi) and the random numbers (zj), j ≠ i, received from the other subscribers according to the equation

$$k: = f(z1, ..., zn),$$

it being required for f to be a symmetrical function which is invariant under the permutation of its arguments.

2. The method for establishing a common key as recited in Claim 1, wherein

a) all subscribers (Ti) involved in the method send the message ($Ni = g^{zi}$) they have generated to a subscriber such as the first subscriber (T1) who has previously been determined to carry out the subsequent method step,

b) the first subscriber (T1) encrypts the received messages (Nj) of the other subscribers ($Tj, j \neq 1$) for each subscriber (Tj) individually with his/her random number (z1) to form in each case one transmission key (k^{1j}), the key being also known to the subscriber (Tj) due to the equation $k^{1j} = k^{j1}$,

c) the first subscriber (T1) sends his/her random number (z1) to all other subscribers (Tj) in encrypted form by generating the message (M1j) according to M1j := $E(k^{1j}, z1)$, with $E(k^{1j}, z1)$ being a symmetrical encryption algorithm in which the data record (z1) is encrypted with the common transmission key (k^{1j}), and

d) the common key (k) to be established is determined by each subscriber (Ti) from the values (Ni) and (Nj), $j \neq i$, and the random number (z1) sent by the first subscriber (T1) in encrypted form with the aid of the equation

$$k: = h\ (z1, g^{z2}, ..., g^{zn}),$$

with h (x1, x2, ..., xn) being a function which is symmetrical in the arguments x2, ..., xn.